



[Subscribe to RSS](#)



[Follow me on Twitter](#)



[Join me on Facebook](#)



WE HAVEN'T LOST OUR MAGIC.

Trusteer recognized as a **leader** in Gartner's 2013 Magic Quadrant for Web Fraud Detection **two years in a row.**

Gartner | **Trusteer**

[VIEW THE REPORT >](#)

Krebs on Security

In-depth security news and investigation



- [About the Author](#)
- [Blog Advertising](#)

04
Jun 13

FDIC: 2011 FIS Breach Worse Than Reported

A 2011 hacker break-in at banking industry behemoth **Fidelity National Information Services (FIS)** was far more extensive and serious than the company disclosed in public reports, banking regulators warned FIS customers last month. The disclosure highlights a shocking lack of basic security protections throughout one of the nation's largest financial services providers.



Jacksonville, Fla. based FIS is one of the largest information processors for the banking industry today, handling a range of services from check and credit card processing to core banking functions for more than 14,000 financial institutions in over 100 countries.

The company came under heavy scrutiny from banking industry regulators in the first quarter of 2011, when hackers who had broken into its networks used that access to orchestrate a carefully-timed, multi-million dollar ATM heist. In that attack, the hackers raised or eliminated the daily withdrawal limits for 22 debit cards they'd obtained from FIS's prepaid card network. The fraudsters then cloned the cards and distributed them to co-conspirators who used them to [pull \\$13 million in cash from FIS via ATMs](#) in several major cities across Europe, Russia and Ukraine.

FIS first publicly reported broad outlines of the breach in a [May 3, 2011 filing](#) with the **Securities and Exchange Commission (SEC)**, stating that it had identified "7,170 prepaid accounts may have been at risk and that three individual cardholders' non-public information may have been disclosed as a result of the unauthorized activities." FIS told the SEC it worked with the impacted clients to take appropriate action, including blocking and reissuing cards for the affected accounts. "The Company has taken steps to further enhance security and continues to work with Federal law enforcement officials on this matter," it declared in its filing.

FIS's disclosure to investors cast the breach as limited in scope, saying the break-in was restricted to unauthorized activity at a portion of its network belonging to a small prepaid debit card provider that it acquired in 2007. But bank examiners at the **Federal Deposit Insurance Corp. (FDIC)** who audited FIS's operations in the months following the 2011 breach and again in October 2012 came to a very different conclusion: According to a report that the FDIC sent May 24, 2013 to hundreds of FIS's customer banks and obtained by KrebsOnSecurity, the 2011 breach was much larger than previously reported.

"The initial findings have identified many additional servers exposed by the attackers; and many more instances of the malware exploits utilized in the network intrusions of 2011, which were never properly identified or assessed," the FDIC examiners wrote in a report from October 2012. "As a result, FIS management now recognizes that the security breach events of 2011 were not just a pre-paid card fraud event, as originally maintained, but rather are that of a broader network intrusion."

Indeed, the FDIC's examiners found that there was scarcely a portion of the FIS network that the hackers *did not* touch.

"From review of the previous investigation reports, along with other documentation provided by FIS, examiners and payment card industry experts identified over 2,000 touch points that indicated a broad exposure of internal FIS systems and client related data," the report notes. "These systems include, but are not limited to, the [The New York Currency Exchange ATM network](#), prime core application systems, and various Internet banking, ACH, and wire transfer systems. These touch points also indicated approximately 100 client financial institutions, which appear to have had sensitive data exposed by the attackers."

The investigation confirmed that data exposed and ex-filtrated during the network intrusion included some information of a high risk nature. This information includes numerous documents that would provide valuable intelligence to an attacker and some that could pose an avenue for future attacks. ☐

A screen shot of an excerpt from the FDIC report on security lapses at FIS.

In an emailed statement, FIS maintained that "no client of FIS suffered any monetary loss as a result of the incident, and stressed that the report is based upon a review that was completed in October 2012.

"Since that time, FIS has continued to strengthen its information security and risk position, including investments over two years of \$100 million or more, as part of our goal to provide best-in-class information security and risk management to each of our 14,000-plus clients. We have openly and regularly communicated these initiatives, our progress and results to our clients and shareholders through meetings, monthly updates, quarterly public disclosures, Board materials, educational webinars, and more."

WHAT DOES \$100 MILLION BUY?

Nevertheless, investors may be less than pleased about how FIS is spending its security dollars. The FDIC found that even though FIS has hired a number of incident response firms and has spent more than \$100 million responding to the 2011 breach, the company failed to enact some very basic security mechanisms. For example, the FDIC noted that FIS routinely uses blank or default passwords on numerous production systems and network devices, even though these were some of the same weaknesses that "contributed to the speed and ease with which attackers transgressed and exposed FIS systems during the 2011 network intrusion."

Enterprise vulnerability scans in November 2012, noted over 10,000 instances of default passwords in use within the FIS environment."

"Many FIS systems remain configured with default passwords, no passwords, non-complex passwords, and non-expiring passwords," the FDIC wrote. "Enterprise vulnerability scans in November 2012, noted over 10,000 instances of default passwords in use within the FIS environment."

The bank auditors also found "a high number of unresolved network and application vulnerabilities remain throughout the enterprise.

"The Executive Summary Scan reports from November 2012 show *18,747 network vulnerabilities and over 291 application vulnerabilities* as past due," the report charges.

What's more, investigators probing the breach at FIS may have been denied key clues about the source of the intrusion because FIS incident response personnel wiped many of the compromised systems and put them back on the network before the machines could be properly examined.

"Many systems were re-constituted and introduced back into the production environment before data preservation techniques were applied," the report notes. "Additionally, poor forensic preservation techniques led to numerous servers being re-imaged before analysis was completed and significant logging data was inadvertently destroyed. Several servers, key to the investigation process, were re-introduced into the production environment and subsequently re-compromised due to misconfigured baselines and inadequate security testing outside of corporate policy."

Analysts say FIS's problems almost certainly stem from having to cobble together various networks and systems that it inherited from a long series of corporate acquisitions over the past few years. The FDIC report notes FIS had originally set a target completion date of year-end 2012 for this project, but has since revised the projected completion date to June 30, 2013.

"It appears the extension is necessary due to the immense scale of the project, which consists of approximately 30,000 servers and operating systems, another 30,000 network devices, over 40,000 workstations, 50,000 network circuits, and 28 mainframes running 80 [LPARs](#)," the FDIC examiners wrote. "The vast scope of this project is being addressed in a formal process which requires additional time to complete. Nonetheless, this information asset inventory and risk rating process is critical to effective information security and risk management efforts; and they should have been implemented prior to regulatory intervention."

The FIS Chief Technology Officer (CTO) has 23 years of experience with FIS. Under the CTO's leadership, FIS has completed documenting and publishing secure coding standards and has begun the roll-out of a centrally managed scanning methodology to address secure coding vulnerabilities across FIS developed applications. The FIS CTO will be responsible for overseeing the remediation of the Development and Acquisition findings. FIS plans to prioritize roll-out throughout 2013 and beyond based upon filters such as consumer, business and internet facing applications and is committed to implementing regular status reports and an enterprise level committee during the second quarter of 2013. As part of the new Enterprise Project Management Methodology, FIS has established several Key Process Indicators (KPIs) to be used for the purposes of analyzing quality and stability of new project introduction and execution. These metrics will be summarized and published to business units and other executive audiences with a target deliverable goal of early second quarter of 2013.

Summary of the New and Prior MRAs

Prior MRAs	Status	New MRAs	"Matters Requiring Attention" Section of the Report
#1	Open		Management Matters #1 (page 5).
#2	Closed		
#3	Closed		
#4	Open		Management Matters #2 (page 5).
#5	Closed		
#6	Closed		
#7	Open		Management Matters #3 (page 5).
#8	Open		Information Security Matters # 4 (page 6).
		#1	Management Matters #4 & #5 (page 5).
		#2	Information Security Matters #1, #2, and #3 (page 6).
		#3	Asset Matters #1 & #2 (page 7).
		#4	Application Development Matters #1 & #2 (page 8).

FDIC-ITS-2012

8

An excerpt from the FDIC report on FIS.

MATTERS REQUIRING ATTENTION

In its initial audit in 2011, the FDIC found eight MRAs, or “matters requiring attention.” [Ron Lindhart](#), a former bank examiner for the [Office of the Comptroller of the Currency](#) (OCC), said MRAs are extremely serious matters that financial services firms ignore at their peril. In its Oct. 2012 follow-up report, the FDIC said while FIS had addressed four of the eight MRAs it identified earlier in the year, the agency had since documented an additional four MRAs.

Lindhart called FIS’s eight MRAs a “high average” score on a report card in which high scores are not a mark of achievement.

“I’d say in a typical examination, you might have two or three, maybe four MRAs, so eight is a significant number,” said Lindhart.

Financial institutions that fail to address MRAs in a timely manner and to the satisfaction of the banking regulators can face fines and can even be shut down. But FIS is a service provider — not a bank — and while the company’s role as a core provider for thousands of banks means that it can be audited by regulators, those regulatory agencies can’t levy fines against the company or shut it down directly.

Rather, Lindhart said, the FDIC’s leverage comes from taking their case to FIS’s customers. Perhaps that is why the FDIC’s May 24, 2013 letter attached the report began with the message, “We are sending you this report for your evaluation and consideration in managing your vendor relationship with FIS.”

Translation? Get FIS’s customer banks to pressure FIS and create the fear that they may lose business by not adequately addressing the security weaknesses. “It’s very effective in getting corrective action when the serviced banks find out about the situation,” Lindhart said.

[Julie Conroy](#), a research director with the retail banking practice of **Aite Group**, a Boston-based research and advisory firm, said a major reason FIS is receiving such regulatory scrutiny is that the company is not just a credit card processor: thousands of small financial institutions outsource their entire information technology systems to FIS.

It’s basically outsourced IT infrastructure for these banks, including all of their customer information — names, SSNs, DBAs, account balances — all of that is sitting at FIS

“It’s basically outsourced IT infrastructure for these banks, including all of their customer information — names, SSNs, DBAs, account balances — all of that is sitting at FIS,” Conroy said. “These kinds of security lapses threatens a key part of the trust relationship that these banks have with the core processors, and [the banks] expect state-of-the-art security.”

But [Avivah Litan](#), a fraud analyst for **Gartner Inc.**, said many of FIS’s customer banks are smaller institutions that can’t exactly afford to pick up and move their operations to a competing service provider, such as **Fiserv** or **Jack Henry**.

“It’s very hard for these banks to switch processors,” Litan said. “The pricing is typically the same, but it takes a lot of manpower to test new systems, to stage it and roll it out in a way that doesn’t disrupt your service.”

Litan said for these institutions, switching service providers is akin to the hassle most consumers experience in trying to switch their Internet service from a cable to a DSL provider - only 100 times harder and more expensive.

“So many of these processors neglect security and have awful customer service, in large part because the switching costs are so high that they can get away with it,” Litan said. “There needs to be more heat on these processors, and I think this is a pretty savvy and important move by the regulators.”

CONNECTIONS TO OTHER ATM CASHOUTS?

The \$13 million ATM cashout against FIS in 2011 bears a remarkable resemblance to several similar heists involving organized crime, malware and ATM cashouts. In May 2013, [federal prosecutors in New York unsealed indictments against eight defendants](#) allegedly involved in two separate cyberattacks that used prepaid debit cards to siphon a total of \$50 million from ATMs across the globe; [the first was a breach around Christmas 2012](#) that netted thieves \$5 million from an Indian prepaid network, while the second siphoned \$40 million from a bank in the United Arab Emirates in February 2013.

Meanwhile, the hackers responsible for coordinating the ATM heists, raising the daily withdrawal limits and monitoring the withdrawals were not

named in the New York indictments.

In its emailed statement to KrebsOnSecurity, FIS said the criminal actors involved in 2011 attack on its own networks “are currently the subject of an ongoing federal criminal law enforcement investigation, and several individuals have been arrested and charged with various crimes.” FIS declined to say whether those arrested were involved in the two thefts connected to the New York investigation.

The FIS breach and the two separate incidents encompassed by the New York case are eerily similar to an intricate 2008 attack against **RBS WorldPay**. In that heist, crooks obtained remote access to RBS’s systems, raised the daily withdrawal limit and used 44 counterfeit prepaid cards to suck more than \$9 million from at least 2,100 ATM terminals in 280 cities worldwide.

Federal prosecutors [alleged](#) that the 2008 RBS theft was orchestrated by at least eight men from Estonia and Russia — the alleged ringleader, **Sergei Tsurikov**, was [extradited](#) to face charges in the United States. His trial is pending and much of his case remains sealed.

Another key figure in that case was **Viktor Pleschuk** of St. Petersburg, Russia, who monitored the fraudulent ATM withdrawals remotely and in real-time using compromised systems within the payment card network. Pleschuk and Russian accomplice **Eugene Anikin** were arrested and charged in Russia. Prosecutors asked the court for five- and six-year sentences, but those requests were ignored. In February 2011 (around the time of the FIS breach) Pleschuk and Anikin agreed to plead guilty for their roles in the RBS heist in exchange for [suspended sentences](#) — probation, but no jail time.



FIS said the criminal actors involved in 2011 attack on its own networks “are currently the subject of an ongoing federal criminal law enforcement investigation, and several individuals have been arrested and charged with various crimes.”

Tags: [Aite Group](#), [avivah litan](#), [Eugene Anikin](#), [fdic](#), [Fidelity National Information Services](#), [FIS](#), [fiserv](#), [gartner](#), [Jack Henry](#), [Julie Conroy](#), [OCC](#), [RBS Worldpay](#), [Ron Lindhart](#), [SEC](#), [Sergei Tsurikov](#), [Viktor Pleschuk](#)

This entry was posted on Tuesday, June 4th, 2013 at 12:50 am and is filed under [A Little Sunshine](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. Both comments and pings are currently closed.

142 comments


1.  [last screw](#)
[June 4, 2013 at 2:36 am](#)

Im in IT security incident response industry for quite a while and there is one thing people fail to realize.

The point here is simple: those who attack with high skill, are not engineers nor have studied any computer science at all, yet they excel(!) at writing and debugging C/ASM code. People who build and manage IT infrastructure are educated engineers who think, act, work in predictable ways and with predictable mistakes, they are educated and trained in one way, likewise they solve problems and look into thing in exactly same ways.

Well those who attack think out of the box, they dont have any CS degree, so they will act in ways no engeneer will imagine and has forseen, i have seen this over and over again.

I think its time to seriously push out-of-the-box style thinking into IT security guys, otherwise well be spending hundereds of milions into nothing but paperweight.

- o  [voksalna](#)
[June 4, 2013 at 6:47 am](#)

The problem is you cannot. That type of thinking is either a part of a person’s unique neurochemistry and/or it is developed and nurtured from a very young age. The best they could do is attempt to create a facsimile of that method of thinking based on case studies. Not everybody can “think out of the box”. In fact, most cannot. Of course, now none of this is very original, but back when these sorts of cashouts were first happening, it was. So such predictive thinking now can be possible for things like this. There will always be the next “black swan”.

- o  [Mike](#)
[June 4, 2013 at 9:22 am](#)

The ability to think outside the box has no relation to one’s possession, or lack, of degree. People who perform these types of attacks are generally more out of the box thinkers because it’s a requirement of the job, not because they don’t have a CS degree. Process oriented thinkers don’t exist in that environment, not because they have a CS degree, but because they aren’t a fit within the criminal organization. Correlation does not imply causation. Especially in this case.